(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－109859

(43)公開日　平成11年(1999)４月23日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０９Ｃ	1/00	６５０	Ｇ０９Ｃ	1/00	６５０Ｂ
					６５０Ｚ
Ｇ０６Ｆ	7/58		Ｇ０６Ｆ	7/58	Ａ

審査請求　有　　請求項の数10　ＦＤ　（全 10 頁）

(21)出願番号　特願平9－290350

(22)出願日　平成９年(1997)10月６日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　島田　道雄
東京都港区芝五丁目７番１号　日本電気株式会社内

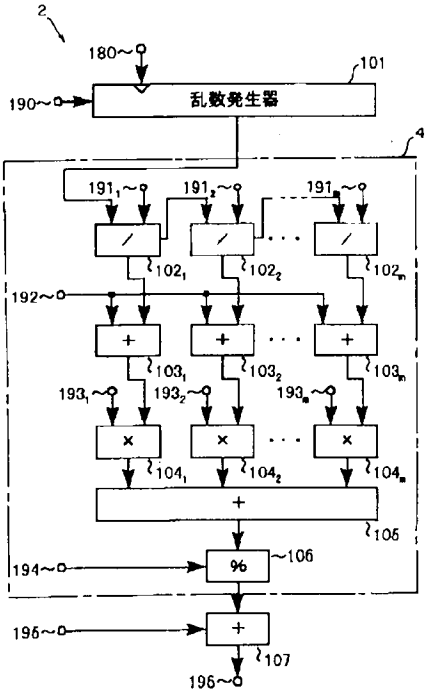
(74)代理人　弁理士　野田　茂

(54)【発明の名称】　擬似乱数発生方法および装置

(57)【要約】

【課題】　素数の候補となる整数を短時間で、かつ低コストで生成する。

【解決手段】　乱数発生器１０１は、入力端子１８０からのクロックパルスに同期して０≦Ａ＜（P_1-1）（P_2-1）……（P_m-1）を満たす整数Ａを無作為に生成する。P_1、P_2、……、P_mは２以上の素数である。第１の演算手段４は、この整数Ａより、式$X=a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$にもとづいて、素数である確率の高い整数Ｘを算出する。ただし、a_k（ｋ＝１、２、……、ｍ）は、合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす整数であり、$B_k$は$\{A \bmod (P_k-1)\}+1$を表す。加算器１０７は、整数Ｘを特定ビット数の整数として出力する。



【特許請求の範囲】

【請求項１】　ｍを正の整数、P_1、P_2、……、P_mを２以上の素数として、与えられた整数（P_1-1）（P_2-1）……（P_m-1）にもとづき、$0 \leqq A < (P_1-1)(P_2-1)\cdots\cdots(P_m-1)$を満たす擬似乱数Ａを乱数発生手段により生成する乱数発生ステップと、

D_kを$D_1=A$で２以上ｍ以下の整数ｋに対して式$D_k=D_{k-1}/(P_k-1)$により表される複数の整数、B_kをｍ以下の正の整数ｋに対して式$\{D_k \bmod (P_k-1)\}+1$により表される複数の整数、ならびにa_kを合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす複数の整数として、式$a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$により表される整数Ｘを除算手段、剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第１の演算ステップと、

ｎを正の整数、Ｑを条件$2^{n-1} \leqq QP_1P_2\cdots\cdots P_m$および$(Q+1)P_1P_2\cdots\cdots P_m \leqq 2^n$を満たす整数として、加算手段により前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算ステップと、

を含むことを特徴とする擬似乱数発生方法。

【請求項２】　前記第１の演算ステップは、$D_1=A$とし２以上ｍ以下の整数ｋに対して整数D_kを整数（P_k-1）によって除したときの商$D_{k+1}=D_k/(P_k-1)$と剰余$D_k \bmod (P_1-1)$を除算手段により算出する除算ステップと、

前記除算ステップで算出した剰余のそれぞれに、第１の加算手段により１を加えて前記複数の整数B_kをそれぞれ算出する第１の加算ステップと、

前記第１の加算ステップで算出した前記複数の整数B_kのそれぞれに、前記乗算手段を用いて対応する整数a_k（$P_1P_2\cdots\cdots P_m/P_k$）を乗じる乗算ステップと、

この乗算ステップにおける乗算結果を第２の加算手段によりすべて加算する第２の加算ステップと、

この第２の加算ステップにおける加算結果を整数$P_1P_2\cdots\cdots P_m$により除したときの剰余を剰余演算手段により算出して前記整数Ｘとする剰余演算ステップと、

を含むことを特徴とする請求項１記載の擬似乱数発生方法。

【請求項３】　ｍを正の整数、ｋをｍ以下の正の整数、P_1、P_2、……、P_mを２以上の素数として、与えられた複数の整数（P_1-1）、（P_2-1）、……、（P_m-1）にもとづき、$0 \leqq A_k < (P_k-1)$を満たす複数の擬似乱数A_kを、複数の乱数発生手段によりそれぞれ生成する乱数発生ステップと、

B_kを式A_k+1により表される複数の整数、ならびにa_kを合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす複数の整数として、式$a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$により表される整数Ｘを剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第１の演算ステップと、

ｎを正の整数、Ｑを条件$2^{n-1} \leqq QP_1P_2\cdots\cdots P_m$および$(Q+1)P_1P_2\cdots\cdots P_m \leqq 2^n$を満たす整数として、加算手段により前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算ステップと、

を含むことを特徴とする擬似乱数発生方法。

【請求項４】　前記第１の演算ステップは、前記乱数発生ステップで生成した前記複数の擬似乱数A_kのそれぞれに、第１の加算手段により１を加えて前記複数の整数B_kをそれぞれ算出する第１の加算ステップと、

前記第１の加算ステップで算出した前記複数の整数B_kのそれぞれに、前記乗算手段を用いて対応する整数a_k（$P_1P_2\cdots\cdots P_m/P_k$）を乗じる乗算ステップと、

この乗算ステップにおける乗算結果を第２の加算手段によりすべて加算する第２の加算ステップと、

この第２の加算ステップにおける加算結果を整数$P_1P_2\cdots\cdots P_m$により除したときの剰余を剰余演算手段により算出して前記整数Ｘとする第２の剰余演算ステップと、

を含むことを特徴とする請求項３記載の擬似乱数発生方法。

【請求項５】　ｍを正の整数、P_1、P_2、……、P_mを２以上の素数として、入力された整数（P_1-1）（P_2-1）……（P_m-1）にもとづいて、$0 \leqq A < (P_1-1)(P_2-1)\cdots\cdots(P_m-1)$を満たす擬似乱数Ａを生成する乱数発生手段と、

D_kを$D_1=A$で２以上ｍ以下の整数ｋに対して式$D_k=D_{k-1}/(P_k-1)$により表される複数の整数、B_kをｍ以下の正の整数ｋに対して式$\{D_k \bmod (P_k-1)\}+1$により表される複数の整数、ならびにa_kを合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす複数の整数として、式$a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$により表される整数Ｘを算出する、除算手段、剰余演算手段、加算手段、ならびに乗算手段を含む第１の演算手段と、

ｎを正の整数、Ｑを条件$2^{n-1} \leqq QP_1P_2\cdots\cdots P_m$および$(Q+1)P_1P_2\cdots\cdots P_m \leqq 2^n$を満たす整数として、前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算手段と、

を含むことを特徴とする擬似乱数発生装置。

【請求項６】　前記第１の演算手段は、

前記擬似乱数Ａに対して$D_1=A$とし、２以上ｍ以下の整数ｋに対して整数D_kを整数（P_k-1）によって除したときの商$D_{k+1}=D_k/(P_k-1)$と剰余$D_k \bmod (P_1-1)$を除算手段により算出する複数の除算手段

と、
前記第１の剰余演算手段で算出した剰余のそれぞれに１を加えて前記複数の整数B_kをそれぞれ算出する複数の第１の加算手段と、
前記第１の加算手段で算出した前記複数の整数B_kのそれぞれに、対応する整数a_k（$P_1P_2\cdots\cdots P_m/P_k$）を乗じる複数の前記乗算手段と、
この乗算手段による乗算結果をすべて加算する第２の加算手段と、
この第２の加算手段による加算結果を整数$P_1P_2\cdots\cdots P_m$により除したときの剰余を算出し、前記整数Ｘとして出力する剰余演算手段と、
を含むことを特徴とする請求項５記載の擬似乱数発生装置。
【請求項７】　ｍを正の整数、ｋをｍ以下の正の整数、P_1、P_2、……、P_mを２以上の素数として、入力された複数の整数（P_1-1）、（P_2-1）、……、（P_m-1）にもとづいて$0 \leqq A_k < (P_k-1)$を満たす複数の擬似乱数A_kをそれぞれ生成する複数の乱数発生手段と、
B_kを式A_k+1により表される複数の整数、ならびにa_kを合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす複数の整数として、式$a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$により表される整数Ｘを算出する、剰余演算手段、加算手段、ならびに乗算手段を含む第１の演算手段と、
ｎを正の整数、Ｑを条件$2^{n-1} \leqq QP_1P_2\cdots\cdots P_m$および$(Q+1)P_1P_2\cdots\cdots P_m \leqq 2^n$を満たす整数として、前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算手段と、
を含むことを特徴とする擬似乱数発生装置。
【請求項８】　前記第１の演算手段は、
前記乱数発生手段で生成した前記複数の擬似乱数A_kのそれぞれに１を加えて前記複数の整数B_kをそれぞれ算出する複数の第１の加算手段と、
前記第１の加算手段で算出した前記複数の整数B_kのそれぞれに、対応する整数a_k（$P_1P_2\cdots\cdots P_m/P_k$）を乗じる複数の前記乗算手段と、
この乗算手段における乗算結果をすべて加算する第２の加算手段と、
この第２の加算手段における加算結果を整数$P_1P_2\cdots\cdots P_m$により除したときの剰余を算出し、前記整数Ｘとして出力する剰余演算手段と、
を含むことを特徴とする請求項７記載の擬似乱数発生装置。
【請求項９】　前記乗算手段はＲＯＭにより構成されていることを特徴とする請求項６または８に記載の擬似乱数発生装置。
【請求項１０】　前記の剰余演算手段は、
第１および第２のＲＯＭと第１および第２の加算器とを含み、
前記第２の加算手段の出力データを構成する複数のビットのうち、下位側の複数のビットは前記第１の加算器の一方の入力端子に供給され、残りのビットは前記第１のＲＯＭのアドレス端子に供給され、前記第１のＲＯＭの出力データは前記第１の加算器のもう一方入力端子に供給されており、
前記第１の加算器の出力データを構成する前記複数のビットのうち、下位側の複数のビットは前記第２の加算器の一方の入力端子に供給され、残りのビットは前記第２のＲＯＭのアドレス端子に供給され、前記第２のＲＯＭの出力データは前記第２の加算器のもう一方入力端子に供給されており、
前記第２の加算器の出力データが前記の剰余演算手段の前記剰余の算出結果として出力されることを特徴とする請求項６または８に記載の擬似乱数発生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は擬似乱数を発生する方法および装置に関するものである。
【０００２】
【従来の技術】従来より、電話、モデム、あるいはテレビジョンなどの通信システムにおける伝送情報が第三者によって盗聴されないようにするため、送信情報に擬似乱数を排他的論理和加算することで送信情報の暗号化が行われている。暗号化の方式には暗号化と復号化とで同一の鍵を用いる慣用暗号と、暗号化と復号化とで異なる鍵を用いる公開鍵暗号の２つの技術が知られている。このうち公開鍵暗号方式は、鍵を通信に先だって予め配送しておく必要がないので手間が省け、また鍵の管理は受信側でのみ行えばよいので鍵の管理が容易であるという利点を有する。
【０００３】公開鍵暗号方式では、受信側は秘密鍵を用いて情報の復号化を行い、この秘密鍵には通常数百ビットから数千ビットもの桁を有する素数が用いられる。したがってこのようなビット数の多い素数を無作為にいかに効率よく生成するかが重要な課題となっている。
【０００４】このような素数の生成には公式が存在しないので、特定のビット数の素数を生成する場合、基本的には、まず特定ビット数の整数を無作為に生成し、それが素数かどうかを判定するということを、素数が得られるまで繰り返す必要がある。しかし、素数か否かを判定するためには多量の計算が必要なため、従来は、単に特定ビット数の整数を無作為に生成するのではなく、素数の候補として、素数である確率の高い整数をまず生成し、その整数に対して素数か否かの判定を行うことで時間の短縮を図っていた。
【０００５】図４はこのような従来の素数の候補を生成

する方法を示すフローチャートである。この図に示すように、まず、ｎを正の整数としてｎビットの整数Ｘ（擬似乱数）を無作為に生成する（手順４１０）。ただし、その整数Ｘが偶数であれば明らかに素数ではなく、また、その整数Ｘは上位ビットが零のためにｎビットでない場合もあるので、その整数Ｘの最下位ビットと最上位ビットを１にする（手順４２０）。次に、正の整数ｊを１とし（手順４３０）、ＸがＰｊで割り切れるかどうかを検査し、ＸがＰｊで割り切れる場合は手順４１０に制御を移し、一方、割り切れない場合は、手順４５０に制御を移す。手順４５０では、ｊ＝ｍか否かを検査し、ｊ＝ｍならば処理を終了してＸを素数の候補（擬似乱数）として出力し、ｊ＝ｍでなければ手順４６０に制御を移す。手順４６０では、ｊ＝ｊ＋１とし、制御を４４０に移す。なお、ここで、ｍは予め決められた正の整数であり、P_1、P_2、……、P_mは互いに異なる小さい素数である。こようにして整数Ｘを生成すれば、Ｘが、P_1、P_2、……、P_m を素因数に持つことがないので、単純に無作為に生成しただけのｎビットの整数よりも素数である確率が高くなり、効率よく特定ビット数の素数を得ることができる。

【０００６】なお、従来の素数生成方法および公開鍵暗号については、例えばシュナイア著「アプライド・クリプトグラフィー（第２版）」（Ｂｒｕｃｅ　Ｓｃｈｎｅｉｅｒ、Ａｐｐｌｉｅｄ　Ｃｒｙｐｔｏｇｒａｐｈｙ：　Ｐｒｏｔｏｃｏｌｓ、Ａｌｇｏｒｉｔｈｍｓ、ａｎｄ　Ｓｏｕｒｃｅ　Ｃｏｄｅ　ｉｎ　Ｃ、ＳｅｃｏｎｄＥｄｉｔｉｏｎ、ＪｏｈｎＷｉｌｅｙ＆Ｓｏｎｓ、Ｉｎｃ．　１９９６）などに詳しく解説されている。

【０００７】

【発明が解決しようとする課題】しかし、無作為に生成されたｎビットの整数が素数である確率は、素数定理からすると、約１／ｎ　程度であることが知られている。したがって、従来の方法では、１つの素数の候補を得るために約ｎ個の整数を無作為に生成する必要があった。そして、秘密鍵としては上述のように数百から数千のビット数の素数が用いられるので、このような秘密鍵の候補を１つ得るために、整数を数百回から数千回も生成し、そのたびに生成した整数を素数Ｐｊで除して整数がＰｊで割り切れるか否かを確認しなければならず、多量の演算を行う必要があった。そのため、素数の候補を得るために時間がかかり、また、除算を実行するために除算器が必要であり、装置は高コストとなっていた。

【０００８】そこで本発明の目的は、素数の候補となる整数を短時間で、かつ低コストで生成できる擬似乱数発生方法および装置を提供することにある。

【０００９】

【課題を解決するための手段】本発明の擬似乱数発生方法は上記目的を達成するため、ｍを正の整数、P_1、P_2、……、P_mを２以上の素数として、与えられた整数（P_1-1）（P_2-1）……（P_m-1）にもとづき、$0 \leqq A < (P_1-1)(P_2-1)\cdots\cdots(P_m-1)$を満たす擬似乱数Ａを乱数発生手段により生成する乱数発生ステップと、D_kを$D_1=A$で２以上ｍ以下の整数ｋに対して式$D_k=D_{k-1}/(P_k-1)$により表される複数の整数、B_kをｍ以下の正の整数ｋに対して式$\{D_k \bmod (P_k-1)\}+1$により表される複数の整数、ならびにa_kを合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす複数の整数として、式$a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$により表される整数Ｘを除算手段、剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第１の演算ステップと、ｎを正の整数、Ｑを条件$2^{n-1} \leqq QP_1P_2\cdots\cdots P_m$および$(Q+1)P_1P_2\cdots\cdots P_m \leqq 2^n$を満たす整数として、加算手段により前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算ステップと、を含むことを特徴とする。

【００１０】また、本発明の擬似乱数発生方法は、ｍを正の整数、ｋをｍ以下の正の整数、P_1、P_2、……、P_mを２以上の素数として、与えられた複数の整数（P_1-1）、（P_2-1）、……、（P_m-1）にもとづき、$0 \leqq A_k < (P_k-1)$を満たす複数の擬似乱数A_kを、複数の乱数発生手段によりそれぞれ生成する乱数発生ステップと、B_kを式A_k+1により表される複数の整数、ならびにa_kを合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす複数の整数として、式$a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$により表される整数Ｘを剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第１の演算ステップと、ｎを正の整数、Ｑを条件$2^{n-1} \leqq QP_1P_2\cdots\cdots P_m$および$(Q+1)P_1P_2\cdots\cdots P_m \leqq 2^n$を満たす整数として、加算手段により前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算ステップと、を含むことを特徴とする。

【００１１】そして、本発明の擬似乱数発生装置は、ｍを正の整数、P_1、P_2、……、P_mを２以上の素数として、入力された整数（P_1-1）（P_2-1）……（P_m-1）にもとづいて、$0 \leqq A < (P_1-1)(P_2-1)\cdots\cdots(P_m-1)$を満たす擬似乱数Ａを生成する乱数発生手段と、$D_k$を$D_1=A$で２以上ｍ以下の整数ｋに対して式$D_k=D_{k-1}/(P_k-1)$により表される複数の整数、$B_k$をｍ以下の正の整数ｋに対して式$\{D_k \bmod (P_k-1)\}+1$により表される複数の整数、ならびに$a_k$を合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす複数の整数として、式$a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$により表される整数Ｘを算出する、除

算手段、剰余演算手段、加算手段、ならびに乗算手段を含む第１の演算手段と、ｎを正の整数、Ｑを条件2^{n-1}≦$QP_1P_2\cdots\cdots P_m$および（Ｑ＋１）$P_1P_2\cdots\cdots P_m$≦2^nを満たす整数として、前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算手段と、を含むことを特徴とする。

【００１２】また、本発明の擬似乱数発生装置は、ｍを正の整数、ｋをｍ以下の正の整数、P_1、P_2、……、P_mを２以上の素数として、入力された複数の整数（P_1-1）、（P_2-1）、……、（P_m-1）にもとづいて０≦A_k＜（P_k-1）を満たす複数の擬似乱数A_kをそれぞれ生成する複数の乱数発生手段と、B_kを式A_k+1により表される前記複数の整数、ならびにa_kを合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす複数の整数として、式$a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$により表される整数Ｘを算出する、剰余演算手段、加算手段、ならびに乗算手段を含む第１の演算手段と、ｎを正の整数、Ｑを条件2^{n-1}≦$QP_1P_2\cdots\cdots P_m$および（Ｑ＋１）$P_1P_2\cdots\cdots P_m$≦2^nを満たす整数として、前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算手段と、を含むことを特徴とする。

【００１３】与えられた任意の非負整数D_kに対して、$\{D_k \pmod{P_k-1}\}+1$で表される上記整数B_kは、０＜B_k＜P_kを満たす。０＜B_k＜P_kであれば、$B_k\neq 0 \pmod{P_k}$である。したがって、P_1、P_2、……、P_mが相異なる素数ならば、連立１次合同式$X=B_1 \pmod{P_1}$、$X=B_2 \pmod{P_2}$、……、$X=B_m \pmod{P_m}$の解が存在し、その解をＸ（上記整数Ｘ）とすると、ＸはP_1、P_2、……、P_mのいずれによっても割り切れない。すなわち、Ｘがｍ個の小さな素数P_1、P_2、……、P_mを素因数に持たないということになり、Ｘが素数である確率は、単に無作為に与えられた整数が素数である確率よりも高くなる。

【００１４】そして、上記連立１次合同式の解Ｘは、$X=a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$によって簡単に求められることが知られており、最初に１つの擬似乱数Ａを生成する本発明の擬似乱数発生方法および装置では、上記第１の演算ステップおよび第１の演算手段において、この式により整数Ｘを算出する。また、上記第２の演算ステップおよび第２の演算手段では、整数Ｘに$QP_1P_2\cdots\cdots P_m$を加算するので、ｎビットの整数が最終出力として得られる。

【００１５】最初に複数の擬似乱数Ａｋを生成する本発明擬似乱数発生方法および装置では、乱数発生ステップおよび乱数発生手段で上記$D_k \pmod{P_k-1}$に相当する擬似乱数A_kを生成し、第１の演算ステップおよび第１の演算手段ではこの擬似乱数A_kにより整数Ｘを算出し、さらに、第２の演算ステップおよび第２の演算手段では上記発明の場合と同様に、ｎビットの整数を生成する。

【００１６】

【発明の実施の形態】次に本発明の実施の形態について図面を参照して説明する。図１は本発明による擬似乱数発生装置の一実施の形態を示す機能ブロック図である。以下ではこの図を参照して本発明による擬似乱数発生装置の一実施の形態について説明し、同時に、対応する本発明による擬似乱数発生方法の一実施の形態について説明する。

【００１７】この擬似乱数発生装置２は、公開鍵暗号方式の秘密鍵とする素数の候補を生成するためのものであり、図１に示したように、本発明に係わる乱数発生手段としての乱数発生器１０１、本発明に係わる第１の演算手段４、本発明に係わる第２の演算手段としての加算器１０７により構成されている。そして、第１の演算手段４は、除算器102_1、102_2、……、102_m（本発明に係わる除算手段）、加算器103_1、103_2、……、103_m（本発明に係わる第１の加算手段）、乗算器104_1、104_2、……、104_m（本発明に係わる乗算手段）、加算器１０５（本発明に係わる第２の加算手段）、剰余演算器１０６（本発明に係わる剰余演算手段）により構成されている。

【００１８】乱数発生器１０１には、入力端子１８０を通じてクロック信号が供給され、一方、入力端子１９０を通じて整数（P_1-1）（P_2-1）……（P_m-1）が入力されている。ここで、ｍは正の整数、P_1、P_2、……、P_mは２以上の素数である。そして、乱数発生器１０１は、上記クロック信号の各クロックパルスに同期して０≦Ａ＜（P_1-1）（P_2-1）……（P_m-1）を満たす擬似乱数Ａを生成し、第１の演算手段４に出力する。

【００１９】第１の演算手段４の機能は、次の［数１］にもとづいて、素数である確率の高い整数Ｘ（擬似乱数）を算出することである。

【００２０】

【数１】$X=a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$

ここで、a_k（ｋ＝１、２、……、ｍ）は、合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす整数である。また、$B_1$、$B_2$、……、$B_k$は、式$B_k=\{D_k \pmod{P_k-1}\}+1$によって値の決められる複数の整数であり、ここで、$D_1$、$D_2$、……、$D_m$は、$D_1$＝Ａ，２以上のｋに対しては$D_k=D_{k-1}/(P_{k-1}-1)$によって値の決められる複数の整数である。

なお、［数１］により表される整数Ｘが、素数である確率が高い整数であることの理由については後に詳しく説明する。

【００２１】第１の演算手段４を構成する各除算器１０２$_k$（ｋ＝１、２、……、ｍ）には、端子１９１$_k$を通じて整数（Ｐ$_k$－１）が入力されて、また、除算器１０２$_1$には、乱数発生器１０１から上記擬似乱数Ａが入力されている。そして、除算器１０２$_1$は擬似乱数Ａを整数（Ｐ$_1$－１）によって除したときの商Ｄ$_2$＝Ａ／（Ｐ$_1$－１）と剰余Ａ　ｍｏｄ　（Ｐ$_1$－１）を算出して、商と剰余を出力し、各除算器１０２$_k$（ｋ＝２，…，ｍ）は、左側の除算器１０２$_{k-1}$の出力する商Ｄ$_k$を整数（Ｐ$_k$－１）によって除したときの商Ｄ$_{k+1}$＝（Ｄ$_k$／（Ｐ$_k$－１）と剰余Ｄ$_k$　ｍｏｄ　（Ｐ$_k$－１）を算出し、商と剰余を出力する。なお、各除算器１０２$_k$（ｋ＝１、２、……、ｍ）の出力する剰余は、それぞれ対応する各加算器１０３$_k$に出力される。なお、以下では説明の便宜上Ｄ$_1$＝Ａと表記する。各加算器１０３$_k$には、各除算器１０２$_k$からの上記剰余と共に、入力端子１９２を通じ″１″が入力されており、各加算器１０３$_k$は剰余Ｄ$_k$　ｍｏｄ　（Ｐ$_k$－１）に１を加え、結果を整数Ｂ$_k$（＝｛Ｄ$_k$　ｍｏｄ　（Ｐ$_k$－１）｝＋１）として対応する各乗算器１０４$_k$に出力する。

【００２２】各乗算器１０４$_k$には、各加算器１０３$_k$による加算結果Ｂ$_k$と共に、各端子１９３$_k$を通じて整数ａ$_k$（Ｐ$_1$Ｐ$_2$……Ｐ$_m$／Ｐ$_k$）が入力されており、乗算器１０４$_k$は、この整数と上記加算結果Ｂ$_k$との積を算出し、結果を加算器１０５に出力する。ここでａ$_k$は、合同式ａ$_k$（Ｐ$_1$Ｐ$_2$……Ｐ$_m$／Ｐ$_k$）＝１　（ｍｏｄ　Ｐ$_k$）を満たす整数である。加算器１０５は、各乗算器１０４$_k$の出力をすべて加算し、加算結果を剰余演算器１０６に出力する。剰余演算器１０６には、この加算結果と共に、端子１９４を通じて素数Ｐ$_1$、Ｐ$_2$、……、Ｐ$_m$の積としての整数Ｐ$_1$Ｐ$_2$……Ｐ$_m$が入力されており、剰余演算器１０６は加算器１０５からの加算結果を整数Ｐ$_1$Ｐ$_2$……Ｐ$_m$で除した時の剰余を算出し、整数Ｘとして加算器１０７に出力する。

【００２３】加算器１０７には、剰余演算器１０６からの整数Ｘと共に入力端子１９５を通じて上記整数Ｐ$_1$Ｐ$_2$……Ｐ$_m$に整数Ｑを乗じた整数ＱＰ$_1$Ｐ$_2$……Ｐ$_m$が入力されており、加算器１０７はこれらの整数を加算し、得られた整数（擬似乱数）を、秘密鍵とする素数の候補として出力する。ここで、Ｑは、条件2^{n-1}≦ＱＰ$_1$Ｐ$_2$……Ｐ$_m$および（Ｑ＋１）Ｐ$_1$Ｐ$_2$……Ｐ$_m$≦2^nを満たす整数である。

【００２４】次に、このように構成された擬似乱数発生装置２の動作について説明する。乱数発生器１０１は、入力端子１８０を通じてクロック信号の１つのクロックパルスが入力されると、そのクロックパルスに同期して０≦Ａ＜（Ｐ$_1$－１）（Ｐ$_2$－１）……（Ｐ$_m$－１）を満たす整数Ａ（擬似乱数）を無作為に生成し、除算器１０２$_1$に供給する（本発明に係わる乱数発生ステップ）。

【００２５】これに対して、除算器１０２$_1$は、擬似乱数Ａを整数（Ｐ$_1$－１）によって除したときの商Ｄ$_2$＝Ａ／（Ｐ$_1$－１）と剰余Ａ　ｍｏｄ（Ｐ$_1$－１）を算出して、商と剰余を出力し、各除算器１０２$_k$（ｋ＝２，…，ｍ）は、左側の除算器１０２$_{k-1}$の出力する商Ｄ$_k$を整数（Ｐ$_k$－１）によって除したときの商Ｄ$_{k+1}$＝Ｄ$_k$／（Ｐ$_k$－１）と剰余Ｄ$_k$　ｍｏｄ　（Ｐ$_k$－１）を算出し、商と剰余を出力し、剰余をそれぞれ対応する加算器１０３$_k$に出力する（本発明に係わる除算ステップ）。なお、以下では説明の便宜上Ｄ$_1$＝Ａと表記する。そして、各加算器１０３$_k$は、各剰余演算器１０２$_k$からの剰余Ｄ$_k$　ｍｏｄ（Ｐ$_k$－１）に、入力端子１９２を通じて入力されている″１″を加え、結果Ｂ$_k$（＝｛Ｄ$_k$　ｍｏｄ　（Ｐ$_k$－１）｝＋１）を対応する乗算器１０４$_k$に出力する（本発明に係わる第１の加算ステップ）。乗算器１０４$_k$は、この加算結果Ｂ$_k$に、対応する入力端子１９３$_k$を通じて入力されている整数ａ$_k$（Ｐ$_1$Ｐ$_2$……Ｐ$_m$／Ｐ$_k$）を乗じ、結果を加算器１０５に出力する（本発明に係わる乗算ステップ）。

【００２６】その後、加算器１０５は、各乗算器１０４$_k$の出力をすべて加算して加算結果を剰余演算器１０６に出力し（本発明に係わる第２の加算ステップ）、剰余演算器１０６は、加算器１０５からの加算結果を、入力端子１９４を通じて入力されている整数Ｐ$_1$Ｐ$_2$……Ｐ$_m$で除した時の剰余を算出して加算器１０７に整数Ｘとして出力する（本発明に係わる剰余演算ステップ）。

【００２７】そして、加算器１０７は、剰余演算器１０６からの上記整数Ｘに、入力端子１９５を通じて入力されている整数ＱＰ$_1$Ｐ$_2$……Ｐ$_m$を加算し、得られた整数（擬似乱数）を、秘密鍵とする素数の候補として出力端子１９６より出力する（本発明に係わる第２の演算ステップ）。［数１］にもとづいて算出された上記整数Ｘは、０≦Ｘ＜Ｐ$_1$Ｐ$_2$……Ｐ$_m$を満たす整数であるから、所望のビット数、すなわちｎビットの整数であるとは限らない。しかし、加算器１０７により、条件2^{n-1}≦ＱＰ$_1$Ｐ$_2$……Ｐ$_m$および（Ｑ＋１）Ｐ$_1$Ｐ$_2$……Ｐ$_m$≦2^nを満たす整数Ｑを整数Ｐ$_1$Ｐ$_2$……Ｐ$_m$に乗じた整数ＱＰ$_1$Ｐ$_2$……Ｐ$_m$を整数Ｘに加算することで、ｎビットの整数が得られる。その結果、入力端子１８０を通じて乱数発生器１０１にクロックパルスが入力されるごとに、公開鍵暗号方式における秘密鍵とするためのｎビットの素数の候補が出力端子１９６を通じて次々に出力される。なお、上記ｍの値は、Ｑの値が存在する範囲でできるだけ大きく選ぶことが、素数である確率がより高い擬似乱数を得る上で好ましい。

【００２８】ここで上記［数１］がいかに導出されるかについて、また、整数Ｘが素数の候補となり得る理由について詳しく説明する。与えられた任意の非負整数Ｄ$_k$

に対して、$B_k=\{D_k \mod (P_k-1)\}+1$で表される上記整数$B_k$は、$0<B_k<P_k$を満たす。$0<B_k<P_k$であれば、$B_k \neq 0 \pmod{P_k}$である。したがって、$P_1$、$P_2$、……、$P_m$が相異なる素数であれば、連立１次合同式$X=B_1 \pmod{P_1}$、$X=B_2 \pmod{P_2}$、……、$X=B_m \pmod{P_m}$の解が存在し、その解をX（上記整数X）とすると、XはP_1、P_2、……、P_mのいずれによっても割り切れない。すなわち、Xがm個の小さな素数P_1、P_2、……、P_mを素因数に持たないということになり、Xが素数である確率は、単に無作為に生成した整数が素数である確率よりも高くなる。

【００２９】そして、上記連立１次合同式の解Xは、$X=a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$によって簡単に求められることが知られており、第１の演算手段４はこの式、すなわち［数１］により整数Xを算出する。

【００３０】このように本実施の形態では、乱数発生器が１つの整数を無作為に生成すると、その整数をもとに所定の演算式（［数１］）にしたがって素数である確率の高い整数、すなわち素数の候補が必ず１つ生成される。したがって、従来のように無作為に多数の整数を生成して素数を選別する方式に比べ極めて短時間で素数の候補を得ることができる。また、従来は素数であるか否かを調べるために除算を行う必要があったが、本実施の形態では除算は不要であり、したがって、除算器を用いることなく低コストで装置を構成することができる。

【００３１】なお、加算器１０７が、剰余演算器１０６からの整数XにQ$P_1P_2\cdots\cdots P_m$を加算する結果、加算器１０７が出力するｎビットの素数の候補（擬似乱数）は、$\{2^{n-1}, \cdots\cdots, 2^n-1\}$の上を一様に分布するのではなく、$\{QP_1P_2\cdots\cdots P_m, \cdots\cdots, (Q+1)P_1P_2\cdots\cdots P_m-1\}$の上を一様に分布することになる。したがって、このｎビットの素数の候補は、統計的には理想的な擬似乱数とは言えないが、本実施の形態では生成した素数の候補を公開鍵暗号の秘密鍵を得るために利用するので、このような場合には十分である。

【００３２】次に、第２の実施の形態について説明する。図２は本発明による擬似乱数発生装置の第２の実施の形態を示す機能ブロック図である。以下ではこの図を参照して本発明による擬似乱数発生装置の第２の実施の形態について説明し、同時に、対応する本発明による擬似乱数発生方法の実施の形態について説明する。なお、図２中、図１と同一の要素には同一の符号が付されており、それらに関する説明はここでは省略する。

【００３３】この擬似乱数発生装置６が図１の擬似乱数発生装置２と異なるのは、図１の乱数発生器１０１が複数の乱数発生器２０１_kにより置き換えられ、そして、第１の演算手段４に相当する第１の演算手段５において各除算器１０２_kが削除されている点である。すなわち、この擬似乱数発生装置６では、各加算器１０３_kに対応して乱数発生器２０１_kが設けられ、各乱数発生器２０１_kには入力端子１８０を通じてクロック信号が入力され、また、各乱数発生器２０１_kに対応する入力端子２９０_kを通じて整数（P_k-1）が供給されている。そして、各乱数発生器２０１_kは、クロック信号の各クロックパルスが入力されるごとに、$0 \leqq A_k < (P_k-1)$を満たす擬似乱数A_kを生成し、対応する加算器１０３_kに出力する。そして、この擬似乱数発生装置６では、各乱数発生器２０１_kが、上記除算器１０２_k（図１）が出力する整数$D_k \mod (P_k-1)$に相当する擬似乱数A_kを生成し、加算器１０３_k以降の各部は上記実施の形態の場合と同様に動作して、ｎビットの整数を素数の候補として生成する。したがって、この実施の形態でも、上記実施の形態の場合と同様の効果が得られ、さらに、この実施の形態では乱数発生器の数は増すものの、m個の除算器が不要になるので、上記実施の形態より一層高速に素数の候補を生成することができる。

【００３４】次に、第３の実施の形態について説明する。図３は本発明による擬似乱数発生装置の第３の実施の形態を示す機能ブロック図である。以下ではこの図を参照して本発明による擬似乱数発生装置の第３の実施の形態について説明し、同時に、対応する本発明による擬似乱数発生方法の実施の形態について説明する。なお、図３中、図２と同一の要素には同一の符号が付されており、それらに関する説明はここでは省略する。

【００３５】この擬似乱数発生装置８が図２の擬似乱数発生装置６と異なるのは、図２の各乗算器１０４_kがそれぞれＲＯＭ（リード・オンリ・メモリ）３０１_kにより置き換えられ、また、剰余演算器１０６が、加算器３０３_1、３０３_2およびＲＯＭ３０２_1、３０２_2により置き換えられている点である。まず、各$ＲＯＭ３０１_k$のアドレス端子には各加算器１０３_kの加算結果が入力され、各$ＲＯＭ３０１_k$のデータ出力端子からは各$ＲＯＭ３０１_k$が保持しているデータが加算器１０５に供給されている。そして、各$ＲＯＭ３０１_k$のｙ番地には（ｙは非負整数）、整数a_k（$P_1P_2\cdots\cdots P_m/P_k$）ｙの値がデータとして書き込まれており、したがって、各$ＲＯＭ３０１_k$は各乗算器１０４_kと同じ機能を果たす。各加算器１０３_kから各$ＲＯＭ３０１_k$に入力されるのは整数B_kであり、この値は小さい。したがって、各$ＲＯＭ３０１_k$のアドレスの最大値も小さくてよく、記憶容量の小さいＲＯＭを用いることができるので、このような構成は容易に実現できる。

【００３６】一方、加算器１０５の出力データを構成する複数のビットのうち、下位側のｎビットは加算器３０３_1の一方の入力端子に、残りのビットは$ＲＯＭ３０２_1$のアドレス端子にそれぞれ供給され、$ＲＯＭ３０２_1$の出力データは加算器３０３_1のもう一方入力端子に供給

されている。また、加算器３０３$_1$の出力データを構成する複数のビットのうち、下位側のｎビットは加算器３０３$_2$の一方の入力端子に、残りのビットはＲＯＭ３０２$_2$のアドレス端子にそれぞれ供給され、ＲＯＭ３０２$_2$の出力データは加算器３０３$_2$のもう一方入力端子に供給されている。

【００３７】そして、各ＲＯＭ３０２$_1$、３０２$_2$のｚ番地（ｚは非負整数）に、整数$2^n z$（ｍｏｄ　$P_1P_2\cdots\cdots P_m$）の値がデータとして書き込まれており、その結果、これら加算器３０３$_1$、３０３$_2$およびＲＯＭ３０２$_1$、３０２$_3$は剰余演算器１０６の機能を果たし、加算器３０３$_2$からは整数Ｘが出力される。各ＲＯＭ３０２$_1$、３０２$_2$に入力される整数ｚは高々ｍであり、ｍの値は小さいので、記憶容量の小さいＲＯＭを用いることができ、このような構成は容易に実現できる。

【００３８】この第３の実施の形態では、上述した擬似乱数発生装置６の場合と同様の効果が得られ、さらに、乗算器および剰余演算器を用いないので、さらに高速に素数の候補を生成することができる。なお、この第３の実施の形態では、第２の実施の形態を構成する乗算器および剰余演算器をＲＯＭや加算器で置き換えたが、第１の実施の形態においても同様に乗算器および剰余演算器をＲＯＭや加算器で置き換え、処理の高速化を図ることも無論可能である。

【００３９】

【発明の効果】以上説明したように本発明の擬似乱数発生方法は、ｍを正の整数、P_1、P_2、……、P_mを２以上の素数として、与えられた整数（P_1-1）（P_2-1）……（P_m-1）にもとづき、$0 \leqq A < (P_1-1)(P_2-1)\cdots\cdots(P_m-1)$を満たす擬似乱数Ａを乱数発生手段により生成する乱数発生ステップと、D_kを$D_1=A$で２以上ｍ以下の整数ｋに対して式$D_k=D_{k-1}/(P_k-1)$により表される整数、B_kをｍ以下の正の整数ｋに対して式$\{D_k \bmod (P_k-1)\}+1$により表される複数の整数、ならびにa_kを合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす複数の整数として、式$a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$により表される整数Ｘを剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第１の演算ステップと、ｎを正の整数、Ｑを条件$2^{n-1} \leqq QP_1P_2\cdots\cdots P_m$および$(Q+1)P_1P_2\cdots\cdots P_m \leqq 2^n$を満たす整数として、加算手段により前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算ステップと、を含むことを特徴とする。

【００４０】また、本発明の擬似乱数発生装置は、ｍを正の整数、P_1、P_2、……、P_mを２以上の素数として、入力された整数（P_1-1）（P_2-1）……（P_m-1）にもとづいて、$0 \leqq A < (P_1-1)(P_2-1)\cdots\cdots(P_m-1)$を満たす擬似乱数Ａを生成する乱数発生手段と、$D_k$を$D_1=A$で２以上ｍ以下の整数ｋに対して式$D_k=D_{k-1}/(P_k-1)$により表される整数、Ｂをｍ以下の正の整数ｋに対して式$\{D_k \bmod (P_k-1)\}+1$により表される複数の整数、ならびにa_kを合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす複数の整数として、式$a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$により表される整数Ｘを算出する、剰余演算手段、加算手段、ならびに乗算手段を含む第１の演算手段と、ｎを正の整数、Ｑを条件$2^{n-1} \leqq QP_1P_2\cdots\cdots P_m$および$(Q+1)P_1P_2\cdots\cdots P_m \leqq 2^n$を満たす整数として、前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算手段と、を含むことを特徴とする。

【００４１】すなわち、本発明では、擬似乱数Ａより所定の数式にもとづいて、素数である確率の高い整数Ｘを算出するので、１つの擬似乱数Ａに対して、素数の候補が必ず１つ生成される。したがって、従来のように無作為に多数の整数を生成して素数を選別する方式に比べ極めて短時間で素数の候補を得ることができる。また、従来は素数であるか否かを調べるために除算を行う必要があったが、本発明では除算は不要であり、したがって、除算器を用いることなく低コストで装置を構成することができる。

【００４２】さらに、本発明の擬似乱数発生方法は、ｍを正の整数、ｋをｍ以下の正の整数、P_1、P_2、……、P_mを２以上の素数として、与えられた複数の整数（P_1-1）、（P_2-1）、……、（P_m-1）にもとづき、$0 \leqq A_k < (P_k-1)$を満たす複数の擬似乱数A_kを、複数の乱数発生手段によりそれぞれ生成する乱数発生ステップと、B_kを式A_k+1により表される複数の整数、ならびにa_kを合同式$a_k(P_1P_2\cdots\cdots P_m/P_k)=1 \pmod{P_k}$を満たす複数の整数として、式$a_1(P_1P_2\cdots\cdots P_m/P_1)B_1+a_2(P_1P_2\cdots\cdots P_m/P_2)B_2+\cdots\cdots+a_m(P_1P_2\cdots\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots\cdots P_m}$により表される整数Ｘを剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第１の演算ステップと、ｎを正の整数、Ｑを条件$2^{n-1} \leqq QP_1P_2\cdots\cdots P_m$および$(Q+1)P_1P_2\cdots\cdots P_m \leqq 2^n$を満たす整数として、加算手段により前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算ステップと、を含むことを特徴とする。

【００４３】また、本発明の擬似乱数発生装置は、ｍを正の整数、ｋをｍ以下の正の整数、P_1、P_2、……、P_mを２以上の素数として、入力された複数の整数（P_1-1）、（P_2-1）、……、（P_m-1）にもとづいて$0 \leqq A_k < (P_k-1)$を満たす複数の擬似乱数A_kをそれぞれ生成する複数の乱数発生手段と、B_kを式A_k+1に

より表される前記複数の整数、ならびにa_kを合同式a_k（$P_1P_2\cdots\cdots P_m/P_k$）＝１　（ｍｏｄ　P_k）を満たす複数の整数として、式a_1（$P_1P_2\cdots\cdots P_m/P_1$）$B_1$　＋a_2（$P_1P_2\cdots\cdots P_m/P_2$）$B_2$　＋……＋　a_m（$P_1P_2\cdots\cdots P_m/P_m$）$B_m$　（ｍｏｄ　$P_1P_2\cdots\cdots P_m$）により表される整数Ｘを算出する、剰余演算手段、加算手段、ならびに乗算手段を含む第１の演算手段と、ｎを正の整数、Ｑを条件$2^{n-1}\leqq QP_1P_2\cdots\cdots P_m$および（Ｑ＋１）$P_1P_2\cdots\cdots P_m\leqq 2^n$を満たす整数として、前記整数Ｘに整数$QP_1P_2\cdots\cdots P_m$を加算して整数を生成し、出力する第２の演算手段と、を含むことを特徴とする。

【００４４】すなわち、本発明では、複数の擬似乱数A_kより所定の数式にもとづいて、素数である確率の高い整数Ｘを算出するので、１組みの擬似乱数A_kに対して、素数の候補が必ず１つ生成される。したがって、従来のように無作為に多数の整数を生成して素数を選別する方式に比べ極めて短時間で素数の候補を得ることができる。また、従来は素数であるか否かを調べるために除算を行う必要があったが、本発明では除算は不要であり、したがって、除算器を用いることなく低コストで装置を構成することができる。

【図面の簡単な説明】

【図１】本発明による擬似乱数発生装置の一実施の形態を示す機能ブロック図である。

【図２】本発明による擬似乱数発生装置の第２の実施の形態を示す機能ブロック図である。

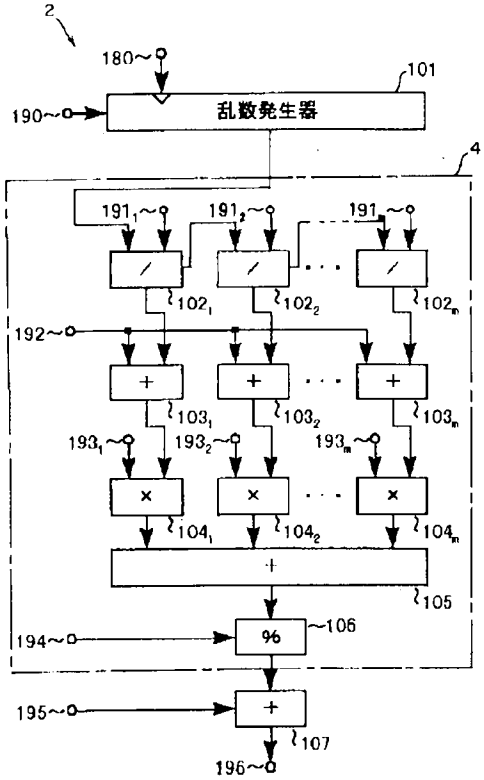
【図３】本発明による擬似乱数発生装置の第３の実施の形態を示す機能ブロック図である。

【図４】従来の素数の候補を生成する方法を示すフローチャートである。

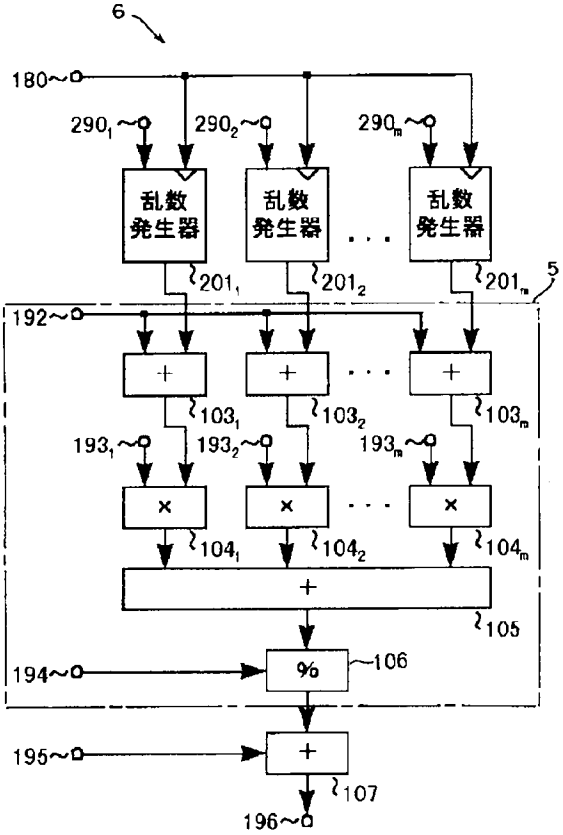
【符号の説明】

２、６、８……擬似乱数発生装置、４、５……第１の演算手段、１０１、201_1、201_2、201_m……乱数発生器、１０５、１０７、103_1、103_2、103_m、302_1、303_2……加算器、１０６、102_1、102_2、102_m……剰余演算器、104_1、104_2、104_m……乗算器、301_1、301_2、301_m、302_1、302_2……ＲＯＭ（リード・オンリ・メモリ）。

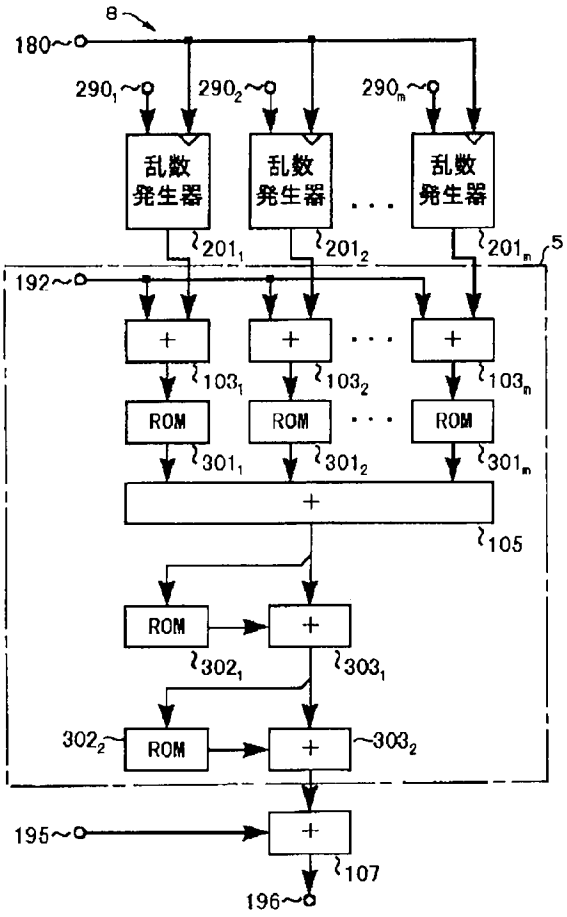
【図１】



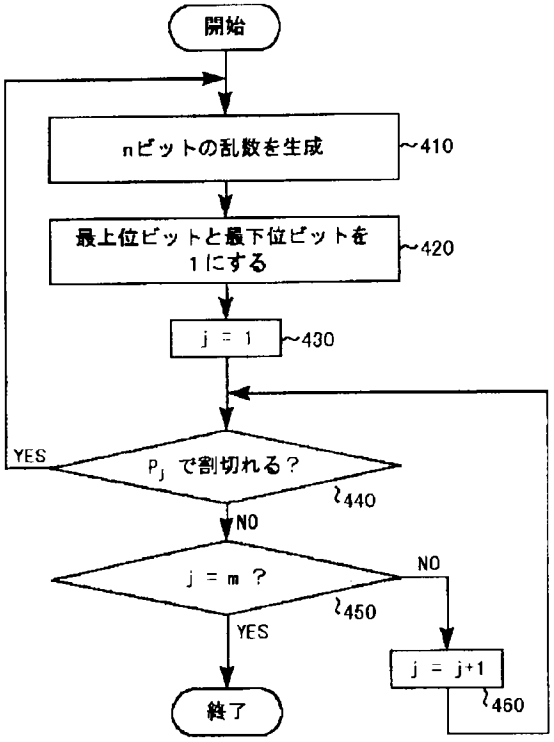
【図２】



【図３】


8
180
290$_1$
290$_2$
290$_m$
乱数発生器
乱数発生器
乱数発生器
201$_1$
201$_2$
201$_n$
5
192
+
103$_1$
103$_2$
103$_n$
ROM
301$_1$
301$_2$
301$_n$
105
302$_1$
303$_1$
302$_2$
303$_2$
195
107
196

【図４】


開始
nビットの乱数を生成
410
最上位ビットと最下位ビットを1にする
420
j = 1
430
YES
P_j で割切れる？
440
NO
j = m ？
450
NO
YES
j = j+1
460
終了

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-109859
(43)Date of publication of application : 23.04.1999

(51)Int.Cl. G09C 1/00
G06F 7/58

(21)Application number : 09-290350
(22)Date of filing : 06.10.1997

(71)Applicant : NEC CORP
(72)Inventor : SHIMADA MICHIO

(54) METHOD FOR GENERATING PSEUDO-RANDOM NUMBER

(57)Abstract:
PROBLEM TO BE SOLVED: To generate an integer which is to be a candidate of a prime number at a low cost in a short time.
SOLUTION: A random number generation unit 101 generates an integer A at random which satisfies 0≤A<(P1−1)(P2−1).....(Pm−1) synchronizing with the clock pulse from input terminal 180. P1P2.....and Pm are prime numbers of two or more. A first operation means 4 calculates an integer Xa prime numberwith a high probability from this integer A based on an expression
X=a1(P1P2.....Pm/P1)B1+a2(P1P2.....Pm/P2)B2+.....+am(P1P2.....Pm/Pm)Bm(mod P1P2.....Pm). Howeverak(k=12...m) is an integer I satisfying a congruence expressionak(P1P2.....Pm/Pk)=1(mod Pk)and Br expresses {A mod (Pk−1)}+1. An adder 107 outputs the integer X as an integer of a specific number of bits.

CLAIMS

[Claim(s)]
[Claim 1]A pseudorandom-numbers generation method comprising:
For m a positive integer$P_1P_2....P_m$ as two or more prime numbersA random number generation step which generates the pseudorandom numbers A which fill 0 <=A<(P_1-1) (P_2-1) .... (P_m-1) by a random number generation means based on given integer (P_1-1) (P_2-1) ---- (P_m-1).
Two or more integers expressed with D_1=A by formula $D_k=D_{k-1}/(P_k-1)$ to the integer k below or more 2m in D_kTwo or more integers expressed by formula $\{D_k \bmod (P_k-1)\}+1$ to positive integer k below m in B_kAnd as two or more integers with which congruence

expression $a_k(P_1P_2 \ldots P_m/P_k) = 1 \pmod{P_k}$ is filleda_kFormula $a_1 \cdot (P_1P_2 \text{ ---- } P_m/P_1) B_1 + a_2(P_1P_2 \ldots P_m/P_2) B_2 + \text{ ---- } + a_m(P_1P_2 \ldots P_m/P_m) B_m$ (.) mod P_1P_2.... The 1st n arithmetic step that computes the integer X expressed by P_m using a division meansa remainder arithmetic meansan adding meansand a multiplication means A positive integerQ Condition $2^{n-1} <= QP_1P_2 \ldots P_m$ and $(Q+1) P_1P_2 \ldots$ It is integer QP_1P_2 to said integer X by an adding means as an integer with which $P_m <= 2^n$ is filled.... The 2nd arithmetic step that adds $P_m$generates an integer and is outputted

[Claim 2]The pseudorandom-numbers generation method comprising according to claim 1:
Said 1st arithmetic stepA division step which computes quotient $D_{k+1}=D_k/(P_k-1)$ when it is referred to as D_1=A and integer D_k is **(ed) for an integer (P_k-1) to the integer k below or more 2mand surplus D_k mod (P_1-1) by a division means.
The 1st summing step that adds 1 to each of a surplus computed at said division step by the 1st adding meansand computes said two or more integer $B_k$respectively.
A multiplication step which multiplies by integer a_k $(P_1P_2 \ldots P_m/P_k)$ which uses said multiplication means for each of two or more of said integer B_k computed by said 1st summing stepand corresponds to it.
The 2nd summing step that adds a multiplication result in this multiplication step altogether by the 2nd adding meansIt is an added result in this 2nd summing step Integer P_1P_2 .... A remainder arithmetic step which computes a surplus when it ** by P_m by a remainder arithmetic meansand is made into said integer X

[Claim 3]A pseudorandom-numbers generation method comprising:
A positive integer below mP_1P_2----and P_m for a positive integer and k as two or more prime numbers[m] being based on two or more given integers $(P_1-1)(P_2-1)$----and (P_m-1) -- $0 <= A_k$ -- $< (P_k-1)$ -- a random number generation step which generates two or more pseudorandom-numbers A_k to fill by two or more random number generation meansrespectively.
Two or more integers expressed by formula A_k+1 in $B_k$and a_k as two or more integers with which congruence expression $a_k(P_1P_2 \text{ ---- } P_m/P_k) = 1 \pmod{P_k}$ is filledFormula $a_1 \cdot (P_1P_2 \text{ ---- } P_m/P_1) B_1 + a_2(P_1P_2 \ldots P_m/P_2) B_2 + \ldots + a_m(P_1P_2 \ldots P_m/P_m) B_m$ (.) mod P_1P_2.... The 1st arithmetic step that computes the integer X expressed by P_m using a remainder arithmetic meansan adding meansand a multiplication meansThey are a positive integer and Q about n Condition $2^{n-1} <= QP_1P_2 \text{ ---- } P_m$ and $(Q+1) P_1P_2$ ---- as an integer with which $P_m <= 2^n$ is filledIt is integer QP_1P_2 to said integer X by an adding means.... The 2nd arithmetic step that adds $P_m$generates an integer and is outputted

[Claim 4]The pseudorandom-numbers generation method comprising according to claim 3:

The 1st summing step that said 1st arithmetic step adds 1 to each of two or more of said pseudorandom-numbers A_k generated at said random number generation step by the 1st adding meansand computes said two or more integer $B_k$respectively.
A multiplication step which multiplies by integer a_k (P_1P_2 .... P_m/P_k) which uses said multiplication means for each of two or more of said integer B_k computed by said 1st summing stepand corresponds to it.
The 2nd summing step that adds a multiplication result in this multiplication step altogether by the 2nd adding means.
It is an added result in this 2nd summing step Integer P_1P_2 .... The 2nd remainder arithmetic step that computes a surplus when it ** by P_m by a remainder arithmetic meansand is made into said integer X

[Claim 5]A pseudorandom-numbers generator comprising:
For m a positive integer$P_1P_2....P_m$ as two or more prime numbersA random number generation means to generate the pseudorandom numbers A which fill 0 <=A<(P_1-1) (P_2-1) .... (P_m-1) based on inputted integer (P_1-1) (P_2-1) ---- (P_m-1).
Two or more integers expressed with D_1=A by formula $D_k=D_{k-1}/(P_k-1)$ to the integer k below or more 2m in D_kIt is a formula to positive integer k below m about B_k. {D_k mod (P_k-1)} Two or more integers expressed by +1And as two or more integers with which congruence expression a_k(P_1P_2 .... P_m/P_k) =1 (mod P_k) is filleda_kFormula a_1. (P_1P_2 ---- P_m/P_1) B_1+a_2(P_1P_2 .... P_m/P_2) B_2+. ---- +a_m(P_1P_2 .... P_m/P_m) B_m (.) mod P_1P_2.... The 1st calculating means including a division meansa remainder arithmetic meansan adding meansand a multiplication means which compute the integer X expressed by P_mThey are a positive integer and Q about n Condition 2^{n-1}<=QP_1P_2 ---- P_m and (Q+1) P_1P_2 ---- as an integer with which P_m<=2^n is filled. It is integer QP_1P_2 to said integer X.... The 2nd calculating means that adds $P_m$generates an integer and is outputted

[Claim 6]The pseudorandom-numbers generator comprising according to claim 5:
Said 1st calculating means is set to D_1=A to said pseudorandom numbers ATwo or more division means which compute quotient $D_{k+1}=D_k/(P_k-1)$ when integer D_k is **(ed) for an integer (P_k-1) to the integer k below or more 2mand surplus D_k mod (P_1-1) by a division means.
Two or more 1st adding means that add 1 to each of a surplus computed by said 1st remainder arithmetic meansand compute said two or more integer $B_k$respectively.
Said two or more multiplication means which multiply by integer a_k (P_1P_2 ---- P_m/P_k) corresponding to each of two or more of said integer B_k computed by said 1st adding means.
It is an added result by the 2nd adding means adding all multiplication results by this multiplication meansand this 2nd adding means Integer P_1P_2 .... A remainder arithmetic means to compute a surplus when it ** by $P_m$and to output as said integer X

[Claim 7]A pseudorandom-numbers generator comprising:
A positive integer below mP_1P_2----and P_m for a positive integer and k as two or more prime numbers[m] being based on two or more integers (P_1-1) and (P_2-1) which were inputted----and (P_m-1) -- $0 <= A_k$ -- $< (P_k-1)$ -- two or more random number generation means to generate two or more pseudorandom-numbers A_k to fillrespectively.
Two or more integers expressed by formula A_k+1 in $B_k$and a_k as two or more integers with which congruence expression $a_k(P_1P_2$ ---- $P_m/P_k) =1$ (mod P_k) is filledFormula a_1. $(P_1P_2$ ---- $P_m/P_1) B_1+a_2(P_1P_2$ .... $P_m/P_2) B_2+$.... $+a_m(P_1P_2$ .... $P_m/P_m) B_m$ (.) mod P_1P_2....
The 1st calculating means including a remainder arithmetic meansan adding meansand a multiplication means which compute the integer X expressed by P_mThey are a positive integer and Q about n Condition $2^{n-1} <= QP_1P_2$ ---- P_m and $(Q+1) P_1P_2$ ---- as an integer with which $P_m <= 2^n$ is filledIt is integer QP_1P_2 to said integer X.... The 2nd calculating means that adds $P_m$generates an integer and is outputted

[Claim 8]The pseudorandom-numbers generator comprising according to claim 7:
Two or more 1st adding means that said 1st calculating means adds 1 to each of two or more of said pseudorandom-numbers A_k generated by said random number generation meansand compute said two or more integer $B_k$respectively.
Said two or more multiplication means which multiply by integer a_k $(P_1P_2$ .... $P_m/P_k)$ corresponding to each of two or more of said integer B_k computed by said 1st adding means.
The 2nd adding means adding all multiplication results in this multiplication means.
It is an added result in this 2nd adding means Integer P_1P_2 .... A remainder arithmetic means to compute a surplus when it ** by $P_m$and to output as said integer X

[Claim 9]The pseudorandom-numbers generator according to claim 6 or 8wherein said multiplication means is constituted by ROM.
[Claim 10]The aforementioned remainder arithmetic means contains the 1st and 2nd ROM and 1st and 2nd adding machinesTwo or more bits by the side of a low rank are supplied to one input terminal of said 1st adding machine among two or more bits which constitute output data of said 2nd adding meansThe remaining bits are supplied to an address terminal of said 1st ROMand output data of said 1st ROM is supplied to an another side input terminal of said 1st adding machineInside of two or more of said bits which constitute output data of said 1st adding machineTwo or more bits by the side of a low rank are supplied to one input terminal of said 2nd adding machineThe remaining bits are supplied to an address terminal of said 2nd ROMand output data of said 2nd ROM is supplied to an another side input terminal of said 2nd adding machineThe pseudorandom-numbers generator according to claim 6 or 8wherein output data of said 2nd adding machine is outputted as a computed result of said

surplus of the aforementioned remainder arithmetic means.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the method and device which generate pseudorandom numbers.
[0002]
[Description of the Prior Art]Beforein order that the transmitted data in communications systemssuch as a telephonea modemor televisionmay not be intercepted by the third partyencryption of transmit information is performed to transmit information by carrying out exclusive OR addition of the pseudorandom numbers. Two art of the public key encryption using a key which is different by the conventional code using the same keyand encryption and decryption by encryption and decryption to the method of encryption is known. Among thesesince time and effort can be saved since the public-key crypto system does not need to deliver a key beforehand in advance of communicationand what is necessary is to perform management of a key only by a receiverit has the advantage that management of a key is easy.
[0003]In a public-key crypto systema receiver decrypts information using a secret key and the prime number which usually has a thousands of [hundreds to] bits beam is used for this secret key. Thereforeit has been an important technical problem how a prime number with much such the number of bits is generated efficiently random.
[0004]When generating the prime number of the specific number of bitsfundamentallythe integer of the number of specific bits is generated at random firstand it is necessary to repeatsince a formula does not exist in generation of such a prime number until a prime number is obtained [judging whether it is a prime number and]. Howeversince a lot of [in order to judge whether it is a prime number] calculations were requiredshortening of time was aimed at by generating first an integer with probability high as a candidate of a prime number which is a prime number rather than only generating the integer of the number of specific bits at randomand judging conventionallythat it is a prime number to the integer.
[0005]Drawing 4 is a flow chart which shows how to generate the candidate of such a conventional prime number. As shown in this figurethe integer X (pseudorandom numbers) of n bit is first generated at random by making n into a positive integer (Procedure 410). Howeversince there is the integer X clearly again not a prime number but when a high order bit is not an n bit because of zero if the integer X is eventhe least significant bit and the most significant bit of the integer X are set to 1 (Procedure 420). Nextpositive integer j is set to 1 (Procedure 430)and it inspects

whether X can divide among $P_j$when X can divide among $P_j$control is moved to Procedure 410and on the other handwhen it cannot be businesslikecontrol is moved to Procedure 450. In Procedure 450it inspects whether it is j=mif j=m becomesprocessing will be endedX will be outputted as a candidate (pseudorandom numbers) of a prime numberand if it is not j=mcontrol will be moved to Procedure 460. In Procedure 460it is considered as j=j+1 and control is moved to 440. m is the positive integer decided beforehand hereand P_m is P_1P_2....a mutually different small prime number. Since P_1P_2....having P_m in a prime factor will not have X if it carries out for coming and the integer X is generatedrather than the integer of n bit generated at random simplythe probability which is a prime number becomes high and the prime number of the number of specific bits can be obtained efficiently.

[0006]About the conventional prime-number-generation method and public key encryption. For exampleSHUNAIA work "applied cryptography (2nd edition)" () [Bruce Schneier and] Applied Cryptography: It explains to ProtocolsAlgorithmsand Source Code in CSecondEditionJohnWiley&SonsInc. 1996etc. in detail.

[0007]

[Problem(s) to be Solved by the Invention]Howeverthe probability that the integer of n bit generated at random is a prime number is about 1/nconsidering a prime number theorem. It is known that it is a grade. Thereforein the conventional methodin order to obtain the candidate of one prime numberabout n integers needed to be generated at random. And since the prime number of thousands of [hundreds to] numbers of bits is used as mentioned above as a secret keyIn order to obtain one candidate of such a secret keyit had to check whether the integer which generated the integer also thousands times from hundreds of timesand was generated at every time would be **(ed) by prime number $P_j$and an integer could divide among $P_j$and a lot of operations needed to be performed. Thereforein order to take time in order to obtain the candidate of a prime numberand to do divisiona divider is requiredand the device had become a high cost.

[0008]Thenthe purpose of this invention is to provide the pseudorandom-numbers generation method and device which are short time and can generate the integer which serves as a candidate of a prime number by low cost.

[0009]

[Means for Solving the Problem]A pseudorandom-numbers generation method of this invention for m a positive integer$P_1P_2....P_m$ in order to attain the above-mentioned purpose as two or more prime numbersBased on given integer (P_1-1) (P_2-1) ---- (P_m-1)A random number generation step which generates the pseudorandom numbers A which fill $0 <= A < (P_1-1)$ (P_2-1) .... (P_m-1) by a random number generation meansTwo or more integers expressed with $D_1=A$ by formula $D_k=D_{k-1}/(P_k-1)$ to the integer k below or more 2m in D_kTwo or more integers expressed by formula $\{D_k \bmod (P_k-1)\}+1$ to positive integer k below m in B_kAnd as two or more integers with which congruence expression $a_k(P_1P_2 .... P_m/P_k) = 1 \pmod{P_k}$ is filleda_kFormula $a_1 . (P_1P_2$ ---- $P_m/P_1)$

$B_1+a_2(P_1P_2 .... P_m/P_2) B_2+ .... +a_m(P_1P_2 .... P_m/P_m) B_m$ (.) mod P_1P_2 .... The 1st arithmetic step that computes the integer X expressed by P_m using a division meansa remainder arithmetic meansan adding meansand a multiplication meansThey are a positive integer and Q about n Condition $2^{n-1}<=QP_1P_2$ ---- P_m and $(Q+1) P_1P_2$ ---- as an integer with which $P_m<=2^n$ is filledIt is integer QP_1P_2 to said integer X by an adding means.... P_m is addedan integer is generated and the 2nd arithmetic step to output is included.

[0010]A pseudorandom-numbers generation method of this invention is provided with the following.

A positive integer below mP_1P_2----and P_m for a positive integer and k as two or more prime numbers[m] being based on two or more given integers $(P_1-1)(P_2-1)$----and (P_m-1) -- 0 $<=A_k$ -- < (P_k-1) -- a random number generation step which generates two or more pseudorandom-numbers A_k to fill by two or more random number generation meansrespectively.

Two or more integers expressed by formula A_k+1 in $B_k$and a_k as two or more integers with which congruence expression $a_k(P_1P_2$ ---- $P_m/P_k) =1$ (mod P_k) is filledFormula a_1. $(P_1P_2$ ---- $P_m/P_1) B_1+a_2(P_1P_2$ ---- $P_m/P_2) B_2+$.... $+a_m(P_1P_2 .... P_m/P_m) B_m$ (.) mod P_1P_2.... The 1st arithmetic step that computes the integer X expressed by P_m using a remainder arithmetic meansan adding meansand a multiplication means

They are a positive integer and Q about n Condition $2^{n-1}<=QP_1P_2$ ---- P_m and $(Q+1) P_1P_2$ .... as an integer with which $P_m<=2^n$ is filledIt is integer QP_1P_2 to said integer X by an adding means.... The 2nd arithmetic step that adds $P_m$generates an integer and is outputted

[0011]And a pseudorandom-numbers generator of this invention is provided with the following.

For m a positive integer$P_1P_2....P_m$ as two or more prime numbersA random number generation means to generate the pseudorandom numbers A which fill 0 $<=A<(P_1-1)$ (P_2-1) .... (P_m-1) based on inputted integer $(P_1-1) (P_2-1)$ ---- (P_m-1).

Two or more integers expressed with $D_1=A$ by formula $D_k=D_{k-1}/(P_k-1)$ to the integer k below or more 2m in D_kIt is a formula to positive integer k below m about B_k. {D_k mod (P_k-1)} Two or more integers expressed by +1And as two or more integers with which congruence expression $a_k(P_1P_2 .... P_m/P_k) =1$ (mod P_k) is filleda_kFormula a_1. $(P_1P_2$ ---- $P_m/P_1) B_1+a_2(P_1P_2 .... P_m/P_2) B_2+$. ---- $+a_m(P_1P_2 .... P_m/P_m) B_m$ (.) mod P_1P_2.... The 1st calculating means including a division meansa remainder arithmetic meansan adding meansand a multiplication means which compute the integer X expressed by P_m

They are a positive integer and Q about n Condition $2^{n-1}<=QP_1P_2$ ---- P_m and $(Q+1) P_1P_2$ .... as an integer with which $P_m<=2^n$ is filledIt is integer QP_1P_2 to said integer X.... The 2nd calculating means that adds $P_m$generates an integer and is outputted

[0012]A pseudorandom-numbers generator of this invention is provided with the

following.
A positive integer below mP_1P_2----and P_m for a positive integer and k as two or more prime numbers[m] being based on two or more integers (P_1-1) and (P_2-1) which were inputted----and (P_m-1) -- 0 <=A_k -- < (P_k-1) -- two or more random number generation means to generate two or more pseudorandom-numbers A_k to fillrespectively.
Said two or more integers expressed by formula A_k+1 in B_kAnd as two or more integers with which congruence expression $ak(P_1P_2$ ---- $P_m/P_k)$ =1 (mod P_k) is filleda$_k$Formula a_1. $(P_1P_2$ ---- $P_m/P_1)$ $B_1+a_2(P_1P_2$ .... $P_m/P_2)$ B_2+. ---- $+a_m(P_1P_2$ ---- $P_m/P_m)$ B_m (.) mod P_1P_2.... The 1st calculating means including a remainder arithmetic meansan adding meansand a multiplication means which compute the integer X expressed by P_m
They are a positive integer and Q about n Condition 2^{n-1}<=QP_1P_2 ---- P_m and (Q+1) P_1P_2 .... as an integer with which P_m<=2^n is filledIt is integer QP_1P_2 to said integer X.... The 2nd calculating means that adds $P_m$generates an integer and is outputted

[0013]The above-mentioned integer B_k expressed with {$D_k$mod} $(P_k-1)+1$ fills $0<B_k<P_k$ to given arbitrary nonnegative integer D_k. It is B_k!=0 if it is $0<B_k<P_k$ (mod P_k). Thereforeif it is P_1P_2....a prime number in which P_m is differentA primary alliance congruence expression If a solution of X= B_1 (mod P_1)X =B_2 (mod P_2)....X=B_m (mod P_m) exists and the solution is set to X (the above-mentioned integer X)X can be divisible by neither P_1 nor P_2 nor .... nor P_m. That ism small prime number P_1P_2....probability that X is a prime number become higher than probability that an integer given only at random [X / it will be said that it does not have P_m in a prime factor and] is a prime number.
[0014]And the solution X of the above-mentioned primary alliance congruence expressionX=a_1. $(P_1P_2$ ---- $P_m/P_1)$ $B_1+a_2(P_1P_2$ .... $P_m/P_2)$ B_2+ ---- $+a_m(P_1P_2$ .... $P_m/P_m)$ B_m (.) mod P_1P_2 .... Asking simply is known by P_m and the integer X is computed by this formula in the 1st arithmetic step of the aboveand the 1st calculating means in a pseudorandom-numbers generation method and a device of this invention which generate the one pseudorandom numbers A first. At the 2nd arithmetic step of the aboveand the 2nd calculating meansit is QP_1P_2 to the integer X.... Since P_m is addedan integer of n bit is acquired as the final output.
[0015]In this invention pseudorandom-numbers generation method and a device which generate two or more pseudorandom numbers Ak to the beginning. Pseudorandom-numbers A_k which is equivalent to above-mentioned D_k mod (P_k-1) by random number generation step and a random number generation means is generatedIn the 1st arithmetic step and 1st calculating meansthe integer X is computed by this pseudorandom-numbers $A_k$and the 2nd arithmetic step and 2nd calculating means generate an integer of n bit like a case of the above-mentioned invention further.
[0016]

[Embodiment of the Invention]Nextan embodiment of the invention is described with reference to drawings. Drawing 1 is a functional block diagram showing the 1 embodiment of the pseudorandom-numbers generator by this invention. Belowwith reference to this figurethe 1 embodiment of the pseudorandom-numbers generator by this invention is describedand the 1 embodiment of the pseudorandom-numbers generation method by corresponding this invention is described simultaneously.
[0017]As it is for this pseudorandom-numbers generator 2 generating the candidate of the prime number used as the secret key of a public-key crypto system and was shown in drawing 1It is constituted by the adding machine 107 as the random number generator 101 as a random number generation means concerning this inventionthe 1st calculating means 4 concerning this inventionand the 2nd calculating means concerning this invention. The 1st calculating means 4 And divider 102_1 102_2....102_m (division means concerning this invention)adding machine 103_1 103_2----103_m (the 1st adding means concerning this invention)It is constituted by multiplier 104_1 104_2....104_m (multiplication means concerning this invention)the adding machine 105 (the 2nd adding means concerning this invention) and the remainder arithmetic machine 106 (remainder arithmetic means concerning this invention).
[0018]a clock signal being supplied to the random number generator 101 through the input terminal 180and leading the input terminal 190 to it on the other hand -- an integer (P_1-1) (P_2-1) .... (P_m-1) is inputted. Herea positive integer$P_1P_2....P_m$ of m are two or more prime numbers. And the random number generator 101 generates the pseudorandom numbers A which fill $0 <= A < (P_1-1)$ (P_2-1) .... (P_m-1) synchronizing with each clock pulse of the above-mentioned clock signaland outputs them to the 1st calculating means 4.
[0019]The function of the 1st calculating means 4 is computing the integer X (pseudorandom numbers) with high probability which is a prime number based on the next [one number].
[0020]
[Equation 1]$X=a_1.(P_1P_2 ---- P_m/P_1)B_1+a_2(P_1P_2 .... P_m/P_2)B_2+ .... +a_m(P_1P_2 .... P_m/P_m)B_m$ (.) mod $P_1P_2 ---- P_m$
Herea_k (k= 12....m) is an integer with which congruence expression $a_k(P_1P_2 ---- P_m/P_k) =1 \pmod{P_k}$ is filled. B_1B_2----and B_kFormula type $B_k= \{D_k \bmod\} (P_k-1)$ By +1are two or more integers values are decided to beand hereD_m is D_1D_2----and two or more integers values are decided to be by $D_k=D_{k-1}/(P_{k-1}-1)$ to $D_1=A$ and two or more k. A reason for probability that the integer X expressed by [an one number] is a prime number being a high integer is explained in detail later.
[0021]An integer (P_k-1) is inputted into each divider 102_k (k= 12....m) which constitutes the 1st calculating means 4 through terminal $191_k$and the above-mentioned pseudorandom numbers A are inputted into divider 102_1 from the random number generator 101. And divider 102_1 computes quotient $D_2=A/(P_1-1)$ when the pseudorandom numbers A are **(ed) for an integer $(P_1-1)$and the surplus A mod $(P_1-$

1)Output a quotient and a surplus and each divider 102 $_k$ (k= 2--m)Quotient D_{k+1}= when quotient D_k which left-hand side divider 102 $_{k-1}$ outputs is **(ed) for an integer (P_k-1) (D_k/(P_k-1) and surplus D_k mod (P_k-1) are computedand a quotient and a surplus are outputted.) A surplus which each divider 102 $_k$ (k= 12....m) outputs is outputted to each adding machine 103 $_k$ correspondingrespectively. Belowit is written as expedient upper D_1=A of explanation. In each adding machine 103 $_k$with the above-mentioned surplus from each divider 102 $_k$. "1" is inputted through the input terminal 192 and each adding machine 103 $_k$ adds one to surplus D_k mod (P_k-1)A result is outputted to each multiplier 104 $_k$ corresponding as integer B_k (= {D_k mod} (P_k-1) +1).

[0022]In each multiplier 104 $_k$with added result B_k by each adding machine 103 $_k$. Integer a_k (P_1P_2 .... P_m/P_k) is inputted through each terminal 193 $_k$and multiplier 104 $_k$ computes a product of this integer and the above-mentioned added result $B_k$and outputs a result to the adding machine 105. a_k is an integer with which congruence expression a_k(P_1P_2 .... P_m/P_k) =1 (mod P_k) is filled here. The adding machine 105 adds all outputs of each multiplier 104 $_k$and outputs an added result to the remainder arithmetic machine 106. In the remainder arithmetic machine 106with this added resultthrough the terminal 194 Prime number P_1P_2----integer P_1P_2 as a product of P_m ---- P_m is inputtedThe remainder arithmetic machine 106 is an added result from the adding machine 105 Integer P_1P_2 .... A surplus when it ** by P_m is computedand it outputs to the adding machine 107 as the integer X.

[0023]The input terminal 195 is led to the adding machine 107 with the integer X from the remainder arithmetic machine 106and it is the above-mentioned integer P_1P_2.... Integer QP_1P_2 which multiplied P_m by the integer Q .... P_m is inputtedThe adding machine 107 outputs an integer (pseudorandom numbers) acquired by adding these integers as a candidate of a prime number used as a secret key. HereQ is condition 2^{n-1}<=QP_1P_2. ---- P_m and (Q+1) P_1P_2 .... It is an integer with which P_m<=2^n is filled.

[0024]Nextoperation of the pseudorandom-numbers generator 2 constituted in this way is explained. If one clock pulse of a clock signal is inputted through the input terminal 180the random number generator 101The integer A (pseudorandom numbers) with which 0 <=A<(P_1-1) (P_2-1) .... (P_m-1) is filled synchronizing with the clock pulse is generated at randomand divider 102 $_1$ is supplied (random number generation step concerning this invention).

[0025]On the other handdivider 102 $_1$ computes quotient D_2=A/(P_1-1) when the pseudorandom numbers A are **(ed) for an integer (P_1-1)and the surplus A mod (P_1-1)Output a quotient and a surplus and each divider 102 $_k$ (k= 2--m)Compute quotient D_{k+1}=D_k/(P_k-1) when quotient D_k which left-hand side divider 102 $_{k-1}$ outputs is **(ed) for an integer (P_k-1)and surplus D_k mod (P_k-1)and a quotient and a surplus are outputtedA surplus is outputted to adding machine 103 $_k$ correspondingrespectively (division step concerning this invention). Belowit is written as expedient upper D_1=A of explanation. And each adding machine 103 $_k$ from each remainder arithmetic machine 102 $_k$ to surplus D_k mod (P_k-1). "1" inputted through the input terminal 192 is

addedand result B_k (= {D_k mod} (P_k−1) +1) is outputted to corresponding multiplier 104 $_k$ (the 1st summing step concerning this invention). Multiplier 104 $_k$ multiplies by integer a_k (P_1P_2 .... P_m/P_k) inputted through input terminal 193 $_k$ corresponding to this added result B_kA result is outputted to the adding machine 105 (multiplication step concerning this invention).

[0026]Thenthe adding machine 105 adds all outputs of each multiplier 104 $_k$outputs an added result to the remainder arithmetic machine 106 (the 2nd summing step concerning this invention)and the remainder arithmetic machine 106Integer P_1P_2 into which an added result from the adding machine 105 is inputted through the input terminal 194 .... A surplus when it ** by P_m is computedand it outputs to the adding machine 107 as the integer X (remainder arithmetic step concerning this invention).

[0027]And integer QP_1P_2 as which the adding machine 107 is inputted into the above-mentioned integer X from the remainder arithmetic machine 106 through the input terminal 195 .... P_m is addedAn acquired integer (pseudorandom numbers) is outputted from the output terminal 196 as a candidate of a prime number used as a secret key (the 2nd arithmetic step concerning this invention). The above-mentioned integer X computed based on [an one number] is 0 <=X<P_1P_2.... Since it is an integer with which P_m is filledit is not necessarily the desired number of bitsi.e.an integer of n bit. With howeverthe adding machine 107. Condition 2^{n-1}<=QP_1P_2 [.... P_m.] ---- P_m and (Q+1) P_1P_2 .... It is the integer Q with which P_m<=2^n is filled Integer P_1P_2 .... Integer QP_1P_2 by which P_m was multiplied An integer of n bit is acquired by adding to the integer X. As a resultwhenever a clock pulse is inputted into the random number generator 101 through the input terminal 180a candidate of a prime number of n bit for considering it as a secret key in a public-key crypto system is outputted one after another through the output terminal 196. When a value of the above-mentioned m obtains pseudorandom numbers with higher probability that it is a prime number to choose in the range in which a value of Q exists as greatly as possibleit is preferred.

[0028]Why the integer X can serve as a candidate of a prime number about how the above [one number] is drawn here is explained in detail. The above-mentioned integer B_k expressed with B_k={$D_k$mod} (P_k−1)+1 fills 0<B_k<P_k to given arbitrary nonnegative integer D_k. It is B_k!=0 if it is 0<B_k<P_k (mod P_k). Thereforeif it is P_1P_2....a prime number in which P_m is differentA primary alliance congruence expression If a solution of X= B_1 (mod P_1)X =B_2 (mod P_2)....X=B_m (mod P_m) exists and the solution is set to X (the above-mentioned integer X)X can be divisible by neither P_1 nor P_2 nor .... nor P_m. That ism small prime number P_1P_2....probability that X is a prime number become higher than probability that an integer generated only at random [X / it will be said that it does not have P_m in a prime factor and] is a prime number.

[0029]And the solution X of the above-mentioned primary alliance congruence expressionX=a_1. (P_1P_2 ---- P_m/P_1) B_1+a_2(P_1P_2 .... P_m/P_2) B_2+ ---- +a_m(P_1P_2 .... P_m/P_m) B_m (.) mod P_1P_2 .... Asking simply is known by P_m and the 1st calculating means 4 computes the integer X by this one formulai.e.a [number].

[0030]Thusaccording to this embodimentif a random number generator generates one integer at randomaccording to a predetermined computing equation ([one number])one candidate of an integer with high probability which is a prime numberi.e.a prime numberwill certainly be generated based on the integer. Thereforecompared with a method which generates many integers at random like beforeand sorts out a prime numbera candidate of a prime number can be obtained extremely in a short time. In order to investigate whether it is a prime number conventionallydivision needed to be donebut division is unnecessarytherefore it can constitute a device from this embodiment by low costwithout using a divider.
[0031]The adding machine 107 is QP_1P_2 from the remainder arithmetic machine 106 to the integer X.... A result adding P_mA candidate (pseudorandom numbers) of a prime number which is n bit which the adding machine 107 outputsIt will not be distributed over Mr. $\{2^{n-1}....2^n-1\}$ top ****but will be distributed over Mr. $\{P_m-QP_1P_2$ .... $P_m....P(Q+1)\ {}_1P_2$ ---- 1} top ****. Thereforealthough he cannot call it ideal pseudorandom numbers statisticallysince a candidate of a prime number of this n bit uses a candidate of a generated prime number in order to obtain a secret key of public key encryptionthis embodiment is enough for him in such a case.
[0032]Nexta 2nd embodiment is described. Drawing 2 is a functional block diagram showing a 2nd embodiment of a pseudorandom-numbers generator by this invention. Belowwith reference to this figurea 2nd embodiment of a pseudorandom-numbers generator by this invention is describedand an embodiment of a pseudorandom-numbers generation method by corresponding this invention is described simultaneously. The same numerals are given to the same element as drawing 1 among drawing 2and explanation about them is omitted here.
[0033]The random number generator 101 of drawing 1 is replaced by two or more random number generator 201 $_k$and that this pseudorandom-numbers generator 6 differs from the pseudorandom-numbers generator 2 of drawing 1 is the point that each divider 102 $_k$ is deleted in the 1st calculating means 5 equivalent to the 1st calculating means 4. Namelyin this pseudorandom-numbers generator 6random number generator 201 $_k$ is provided corresponding to each adding machine 103 $_k$A clock signal is inputted into each random number generator 201 $_k$ through the input terminal 180and an integer (P_k-1) is supplied through input terminal 290 $_k$ corresponding to each random number generator 201 $_k$. and as for each random number generator 201 $_k$each clock pulse of a clock signal is inputted -- alike -- $0 <= A_k -- < (P_k-1)$ -- pseudorandom-numbers A_k to fill is generated and is outputted to corresponding adding machine 103 $_k$. And in this pseudorandom-numbers generator 6 each random number generator 201 $_k$Generating pseudorandom-numbers A_k equivalent to integer D_k mod (P_k-1) which the above-mentioned divider 102 $_k$ (drawing 1) outputseach part after adding machine 103 $_k$ operates like a case of the above-mentioned embodimentand generates an integer of n bit as a candidate of a prime number. Thereforealthough the same effect as a case of the above-mentioned

embodiment is acquired and the number of random number generators also increases this embodiment by this embodiment furthersince m dividers become unnecessarya candidate of a prime number is further generable at a high speed from the above-mentioned embodiment.

[0034]Nexta 3rd embodiment is described. Drawing 3 is a functional block diagram showing a 3rd embodiment of a pseudorandom-numbers generator by this invention. Belowwith reference to this figurea 3rd embodiment of a pseudorandom-numbers generator by this invention is describedand an embodiment of a pseudorandom-numbers generation method by corresponding this invention is described simultaneously. The same numerals are given to the same element as drawing 2 among drawing 3and explanation about them is omitted here.

[0035]That this pseudorandom-numbers generator 8 differs from the pseudorandom-numbers generator 6 of drawing 2Each multiplier 104_k of drawing 2 is replaced by ROM(read only memory) 301_krespectivelyThe remainder arithmetic machine 106 is the point currently replaced by adding machine $303_1$$303_2$ and ROM$302_1$and 302_2. Firstan added result of each adding machine 103_k is inputted into an address terminal of each ROM$301_k$and data which each ROM301_k holds is supplied to the adding machine 105 from a data output terminal of each ROM301_k. (y at y address of each ROM301_k And nonnegative integer)A value of integer $a_k(P_1P_2 \cdots P_m/P_k)$ y is written in as datatherefore each ROM301_k achieves the same function as each multiplier 104_k. Integer B_k is inputted into each ROM301_k from each adding machine $103_k$and this value is small. Thereforesince ROM with the small maximum of an address of each ROM301_k and a small storage capacity can be usedsuch composition is easily realizable.

[0036]On the other handn bit by the side of a low rank among two or more bits which constitute output data of the adding machine 105 to one input terminal of adding machine 303_1. The remaining bits are supplied to an address terminal of ROM302_1respectivelyand output data of ROM302_1 is supplied to an another side input terminal of adding machine 303_1. Inside of two or more bits which constitute output data of adding machine 303_1n bit by the side of a low rank is supplied to one input terminal of adding machine $303_2$the remaining bits are supplied to an address terminal of ROM302_2respectivelyand output data of ROM302_2 is supplied to an another side input terminal of adding machine 303_2.

[0037]At and z address (z is a nonnegative integer) of each ROM302_1 and 302_2. A value of integer $2^nz \pmod{P_1P_2 \cdots P_m}$ is written in as dataAs a resultthese adding machine $303_1$$303_2$ and ROM$302_1$and 302_3 achieve a function of the remainder arithmetic machine 106and the integer X is outputted from adding machine 303_2. the integer z inputted into each ROM302_1 and 302_2 -- at most -- it is mand since a value of m is smallROM with a small storage capacity can be used and such composition can be realized easily.

[0038]According to this 3rd embodimentat still high speedsince the same effect as a

case of the pseudorandom-numbers generator 6 mentioned above is acquired and a multiplier and a remainder arithmetic machine are not used furthera candidate of a prime number can be generated. Although a multiplier and a remainder arithmetic machine which constitute a 2nd embodiment were replaced with ROM or an adding machine in this 3rd embodimentof courseit is also possible to replace a multiplier and a remainder arithmetic machine with ROM or an adding machine similarly in a 1st embodimentand to attain improvement in the speed of processing.

[0039]

[Effect of the Invention]As explained abovethe pseudorandom-numbers generation method of this invention is provided with the following.

For m a positive integer$P_1P_2....P_m$ as two or more prime numbersThe random number generation step which generates the pseudorandom numbers A which fill $0 <=A<(P_1-1)$ (P_2-1) .... (P_m-1) by a random number generation means based on given integer (P_1-1) (P_2-1) ---- (P_m-1).

The integer expressed with $D_1=A$ by formula $D_k=D_{k-1}/(P_k-1)$ to the integer k below or more 2m in D_kTwo or more integers expressed by formula $\{D_k \bmod (P_k-1)\}+1$ to positive integer k below m in B_kAnd as two or more integers with which congruence expression $a_k(P_1P_2 .... P_m/P_k) =1 \pmod{P_k}$ is filleda_kFormula $a_1. (P_1P_2 ---- P_m/P_1) B_1+a_2(P_1P_2 .... P_m/P_2) B_2+. ---- +a_m(P_1P_2 .... P_m/P_m) B_m$ (.) modP_1P_2.... The 1st arithmetic step that computes the integer X expressed by P_m using a remainder arithmetic meansan adding meansand a multiplication means

They are a positive integer and Q about n Condition $2^{n-1}<=QP_1P_2 ---- P_m$ and $(Q+1)$ P_1P_2 .... as an integer with which $P_m<=2^n$ is filledIt is integer QP_1P_2 to said integer X by an adding means.... The 2nd arithmetic step that adds $P_m$generates an integer and is outputted

[0040]The pseudorandom-numbers generator of this invention is provided with the following.

For m a positive integer$P_1P_2....P_m$ as two or more prime numbersA random number generation means to generate the pseudorandom numbers A which fill $0 <=A<(P_1-1)$ (P_2-1) .... (P_m-1) based on inputted integer (P_1-1) (P_2-1) ---- (P_m-1).

The integer expressed with $D_1=A$ by formula $D_k=D_{k-1}/(P_k-1)$ to the integer k below or more 2m in D_kTwo or more integers expressed by formula $\{D_k \bmod\} (P_k-1)+1$ to positive integer k below m in BAnd as two or more integers with which congruence expression $a_k(P_1P_2 .... P_m/P_k) =1 \pmod{P_k}$ is filleda_kFormula $a_1. (P_1P_2 ---- P_m/P_1) B_1+a_2(P_1P_2 .... P_m/P_2) B_2+. ---- +a_m(P_1P_2 ---- P_m/P_m) B_m$ (.) mod P_1P_2.... The 1st calculating means including the remainder arithmetic meansadding meansand multiplication means which compute the integer X expressed by P_m

They are a positive integer and Q about n Condition $2^{n-1}<=QP_1P_2 ---- P_m$ and $(Q+1)$ P_1P_2 .... as an integer with which $P_m<=2^n$ is filledIt is integer QP_1P_2 to said integer X.... The 2nd calculating means that adds $P_m$generates an integer and is outputted

[0041]That isin this inventionsince the integer X with high probability which is a prime number is computed based on predetermined expression from the pseudorandom numbers Aone candidate of a prime number is certainly generated to the one pseudorandom numbers A. Thereforecompared with the method which generates many integers at random like beforeand sorts out a prime numberthe candidate of a prime number can be obtained extremely in a short time. In order to investigate whether it is a prime number conventionallydivision needed to be donebut division is unnecessarytherefore it can constitute a device from this invention by low costwithout using a divider.

[0042]The pseudorandom-numbers generation method of this invention is provided with the following.

The positive integer below mP_1P_2----and P_m for a positive integer and k as two or more prime numbers[m] being based on two or more given integers (P_1-1)(P_2-1)---- and (P_m-1) -- 0 <=A_k -- < (P_k-1) -- the random number generation step which generates two or more pseudorandom-numbers A_k to fill by two or more random number generation meansrespectively.

Two or more integers expressed by formula A_k+1 in $B_k$and a_k as two or more integers with which congruence expression a_k(P_1P_2 ---- P_m/P_k) =1 (mod P_k) is filledFormula a_1. (P_1P_2 ---- P_m/P_1) B_1+a_2(P_1P_2 ---- P_m/P_2) B_2+.... +a_m(P_1P_2 .... P_m/P_m) B_m (.) mod P_1P_2.... The 1st arithmetic step that computes the integer X expressed by P_m using a remainder arithmetic meansan adding meansand a multiplication means

They are a positive integer and Q about n Condition 2^{n-1}<=QP_1P_2 ---- P_m and (Q+1) P_1P_2 .... as an integer with which P_m<=2^n is filledIt is integer QP_1P_2 to said integer X by an adding means.... The 2nd arithmetic step that adds $P_m$generates an integer and is outputted

[0043]The pseudorandom-numbers generator of this invention is provided with the following.

The positive integer below mP_1P_2----and P_m for a positive integer and k as two or more prime numbers[m] being based on two or more integers (P_1-1) and (P_2-1) which were inputted----and (P_m-1) -- 0 <=A_k -- < (P_k-1) -- two or more random number generation means to generate two or more pseudorandom-numbers A_k to fillrespectively.

Said two or more integers expressed by formula A_k+1 in B_kAnd as two or more integers with which congruence expression a_k(P_1P_2 .... P_m/P_k) =1 (mod P_k) is filleda$_k$Formula a_1. (P_1P_2 ---- P_m/P_1) B_1+a_2(P_1P_2 .... P_m/P_2) B_2+. ---- +a_m(P_1P_2 ---- P_m/P_m) B_m (.) mod P_1P_2.... The 1st calculating means including the remainder arithmetic meansadding meansand multiplication means which compute the integer X expressed by P_m

They are a positive integer and Q about n Condition 2^{n-1}<=QP_1P_2 ---- P_m and (Q+1)

P_1P_2 .... as an integer with which $P_m <= 2^n$ is filledIt is integer QP_1P_2 to said integer X.... The 2nd calculating means that adds $P_m$generates an integer and is outputted

[0044]That isin this inventionsince the integer X with high probability which is a prime number is computed based on predetermined expression from two or more pseudorandom-numbers $A_k$one candidate of a prime number is certainly generated to pseudorandom-numbers A_k constructed one. Thereforecompared with the method which generates many integers at random like beforeand sorts out a prime numberthe candidate of a prime number can be obtained extremely in a short time. In order to investigate whether it is a prime number conventionallydivision needed to be donebut division is unnecessarytherefore it can constitute a device from this invention by low costwithout using a divider.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a functional block diagram showing the 1 embodiment of the pseudorandom-numbers generator by this invention.
[Drawing 2]It is a functional block diagram showing a 2nd embodiment of the pseudorandom-numbers generator by this invention.
[Drawing 3]It is a functional block diagram showing a 3rd embodiment of the pseudorandom-numbers generator by this invention.
[Drawing 4]It is a flow chart which shows how to generate the candidate of the conventional prime number.
[Description of Notations]
268 .... A pseudorandom-numbers generator45 ---- The 1st calculating means101201 $_1$201 $_2$201 $_m$ .... A random number generator105 and 107103 $_1$103 $_2$103 $_m$302 $_1$303 $_2$ .... Adding machine106102 $_1$102 $_2$102 $_m$ .... Remainder arithmetic machine104 $_1$104 $_2$104 $_m$ .... A multiplier301 $_1$301 $_2$301 $_m$302 $_1$302 $_2$ ---- ROM (read only memory).
